What is claimed is:

1. A computerized system for encrypting an electronic message between a sender and a recipient regardless of whether the sender or recipient are members of an encryption system comprising:

a computer processor;

a computer readable medium in communications with said computer processor;

a communications link for communications between said computer readable medium, a sender's terminal and a recipients terminal;

a set of non-member computer readable instructions contained within said computer readable medium, when processed by a computer processor and in response to a member sending an electronic message to a non-member recipient from said sender terminal:

prompting the member for an encryption pass-phrase at said sender terminal,

receiving an encryption pass-phrase from the member at said sender terminal,

generating an encryption key pair,

encrypting the electronic message responsive to said encryption key pair so that said key pair may be used to decrypt said encrypted message,

sending a notification to said recipient terminal that an encrypted message is available to the non-member recipient,

encrypting said encryption key pair according to said encryption pass-phrase,

prompting the non-member for a decryption pass-phrase corresponding to said encrypted message at said recipient ,

receiving said decryption pass-phrase from the non-member,

decrypting said encrypted key pair in response to receiving a decryption pass-phrase corresponding to said encryption pass-phrase,

decrypting said encrypted message according to said encryption key pair, and,

providing the decrypted message for review to said non-member so that the non-member can receive and decrypt an electronic message from a member of an encryption system even though the non-member is not a member of the encryption system.

2. The system of claim 1 wherein said set of non-member instructions includes instructions for:

removing said unencrypted key pair from said computer readable medium; and,

removing said encryption pass-phrase from said computer readable medium so that only said encrypted encryption key pair is contained within said computer readable medium.

3. The system of claim 1 including:

a member database contained within said computer readable medium having a member record associated with each of the members of the encryption system;

a set of member location instructions contained within said computer readable medium for:

querying said member database for determining whether the recipient has an associated record within said member database, and,

executing said non-member instructions if no associated record is found for the recipient in said member database.

4. The system of claim 1 wherein said non-member encryption instructions includes instruction for:

prompting the member at said sender terminal for a message lifetime value;

associating said message lifetime value with the encrypted message send by the member; and,

a set of lifetime deletion instructions contained within said computer readable medium for deleting said encrypted message upon expiration of said lifetime value associated with the electronic message so that upon expiration of said lifetime value the electronic message can not be decrypted and therefore is unavailable for review.

5. The system of claim 1 including:

a message database included within said computer readable medium having a message record associated with the electronic message; and,

said non-member instructions including instructions for:

creating a message ID associated with said electronic message to be sent to the non-member,

storing said message ID within said message record associated with the electronic message, and,

storing said encrypted encryption key pair within said message record associated with the electronic message.

6. The system of claim 1 including a set of stale message instructions contained within said computer readable medium for deleting said encryption key pair associated with said encrypted message upon the expiration of a predetermined period of time so that if the encrypted message is not decrypted within said predetermined period of time, the encrypted message is unavailable for review.

7. The system of claim 1 wherein:

said non-member instructions include instruction for:

prompting the member at said sender terminal for a message lifetime value,

associating said lifetime value with the encrypted message sent by the member, and,

a set of lifetime deletion instructions contained within said computer readable medium for deleting said encryption key pair upon expiration of said lifetime

value associated with the electronic message so that upon expiration of said lifetime value the electronic message can not be decrypted and therefore is unavailable for review.

8. The system of claim 1 including deletion instructions contained within said computer readable medium for deleting said encryption key pair upon receiving a delete request from the non-member so that the non-member can expressly request the encrypted message be made unavailable for review.

9. The system of claim 1 including:

a member database contained within said computer readable medium having a member record associated with each of the members of the encryption system;

a unique public key contained within said member record associated with each of the members of said encryption system; and,

a set of reply instructions contained with said computer readable medium in response to receiving a reply command from the non-member recipient through said recipient terminal for:

receiving a reply message from the non-member recipient intended for the sending member;

retrieving said unique public key associated with the sending member from said member database;

encrypting said reply message according to said unique public key of the sending member; and,

informing said sending member that an encrypted reply message from the non-member is available for decrypting and review by the member so that a non-member can send an encrypted reply to a member of an encryption system without having to be a member of that encryption system.

10. The system of claim 1 including:

a member database contained within said computer readable medium having a member record associated with each of the members of the encryption system;

a unique private key contained within said member record associated with each of the members of the encryption system;

a set of member instructions contained within said computer readable medium in response to a first member sending an electronic message to a second member for:

retrieving a second member's public key from said member database,

encrypting said electronic message responsive to said second member's public key; and,

sending a notification to the second member notifying the second member that an encrypted message is available for decryption so that an electronic message is encrypted automatically and the receiving member is notified automatically when an encrypted message is available for decryption and review.

11. The system of claim 10 wherein said member instructions include instructions in response to the second member requesting to decrypt the encrypted message for:

retrieving a second member's private key from said member database;

decrypting the encrypted electronic message from the first member according to said second member's private key; and,

providing said decrypted electronic message to the second member for review so that an electronic message can be encrypted, sent from a first member to a second member, and decrypt automatically.

12. A computerized system for encrypting an electronic message between a sender and a recipient regardless of whether the sender or recipient are members of an encryption system embodied in a computer readable medium comprising:

a means for receiving input from the sender including an encryption pass-phrase associated with an electronic message;

a means for generating an encryption key pair for encrypting the message;

a means for encrypting the electronic message responsive to said encryption key pair so that said key pair may be used to decrypt said encrypted message;

a means for encrypting said encryption key pair according to said encryption pass-phrase;

a means for notifying a recipient non-member that an encrypted message is available to the non-member for decryption and review;

a means for receiving a decryption pass-phrase from the non-member;

a means for decrypting said encrypted encryption key pair in response to receiving a decryption pass-phrase corresponding to said encryption pass-phrase associated with the electronic encrypted message;

a means for decrypting said encrypted message according to said decrypted encryption key pair; and,

a means for providing the decrypted message to the recipient non-member so that the non-member can receive and decrypt an electronic message from a member of an encryption system even though the non-member is not a member of the encryption system.

13. The system of claim 12 including:

a means for receiving a message lifetime value from the sender;

a means for associating said message lifetime value with the encrypted message sent by the sending member; and,

a means for deleting said encrypted message upon expiration of said lifetime value associated with the electronic message so that upon expiration of said lifetime value the electronic message can not be decrypted and therefore is unavailable for review.

14. The system of claim 12 including a means for deleting said encryption key pair associated with said encrypted message upon the expiration of a

predetermined period of time so that if the encrypted message is not decrypted within said predetermined period of time, the encrypted message is unavailable for review.

15. The system of claim 12 including a means for deleting said encryption key pair upon receiving a delete request from said non-member so that the non-member can expressly request for the encrypted message to be made unavailable for review.

16. The system of claim 12 including:

a means for receiving a reply message from the non-member intended for the sending member;

a means for encrypting said reply message; and

a means for informing the sending member that an encrypted reply message from the non-member is available for decrypting and review by the member so that a non-member can send an encrypted reply to a member of an encryption system without having to be a member of that encryption system.

17. The system of claim 12 including:

a means for encrypting an electronic message sent between a first member and a second member of an electronic encryption system; and,

a means for sending a notification to the second member notifying the second member that an encrypted message is available for decryption so that an electronic message is encrypted automatically and the receiving member is notified automatically when an encrypted message is available for decryption and review.

18. The system of claim 17 including a means for decrypting the encrypted

electronic message from the first member according to a decryption request from the second member so that an electronic message can be encrypted, sent from a first member to a second member, and decrypted automatically.

19. The system of claim 12 including:

a means for receiving a message lifetime value from the sender;

a means for associating said lifetime value with the encrypted message sent by the sending member; and,

a means for deleting said encryption key pair upon expiration of said lifetime value so that upon the expiration of said lifetime value, the electronic message can not be decrypted with said encryption keys.

20. The system of claim 12 including a means for deleting said encrypted message so that if said encrypted message is not decrypted within prescribed a period of time, the message is unavailable for review.

21. The method for encrypting an electronic message between a sender and a recipient regardless of whether the sender or recipient are members of the encryption system comprising the steps of:

receiving the electronic message supplied by the sender to be sent to the recipient;

receiving an encryption pass-phrase supplied by the sender;

generating an encryption key pair associated with the message to be encrypted;

encrypting the message according to said encryption key pair so that

said key pair may be used to decrypt the encrypted message;

sending a notification to the recipient that an encrypted message is available to the recipient for review; and,

encrypting said encryption key pair according to said encryption pass-phrase.

22. The method of claim 21 including the steps of:

receiving a decryption pass-phrase supplied by the recipient;

decrypting said encrypted key pair in response to receiving a decryption pass-phrase corresponding to said encryption pass phrase;

decrypting said encrypted message according to said encryption key pair; and,

providing the decrypted message for review to the recipient so that the non-member can retrieve and decrypt the electronic message from a sender of an encryption system even though the recipient is not a member of the encryption system.

23. The method of claim 21 including the steps of:

destroying said unencrypted encryption key pair after encrypting said key pair; and,

destroying said encryption pass-phrase so that only said encrypted encryption key pair is remaining.

24. The method of claim 21 including the steps of:

prompting the sender for a message lifetime value;

associating said message lifetime value with the encrypted message;

and,

deleting said encrypted message upon said expiration of said lifetime value so that upon expiration of said lifetime value, the electronic message unavailable for review.

25. The method of claim 21 including the steps of deleting said encryption key pair associated with said encryption message upon the expiration of the predetermined period of time so that if the encrypted message is not decrypted within said predetermined period of time, the encrypted message is unavailable for review.

26. The method of claim 21 including deleting said encryption key pair upon receiving a delete request from the recipient so that the recipient can expressly request for an encrypted message to made unavailable for review.

27. The method of claim 21 including the steps of: providing a unique public key associated with the sender;

receiving a reply message from the recipient intended for the sender;

encrypting said reply message according to said unique public key;

and,

informing the sender that the encrypted reply message from the recipient is available for review.

28. The method of claim 21 including:

supplying a unique public key associated with recipient;

encrypting the electronic message responsive to said recipient's public key; and,

sending a notification to the recipient notifying the recipient that an encrypted message is available for decryption and review.

29. The method of claim 28 including:

supplying a unique private key associated with the recipient;

decrypting the encrypted electronic message from the sender according to said recipient's private key; and,

providing said decrypted electronic message to the recipient for review.